

CVE-2019-11580

Atlassian Crowd and Crowd Data Center Remote Code Execution Vulnerability

Exigent CISA KEV since Nov 3, 2021 Actively exploited Ransomware use known Public exploit module (Metasploit)

Atlassian Crowd and Crowd Data Center had the pdkinstall development plugin incorrectly enabled in release builds. Attackers who can send unauthenticated or authenticated requests to a Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permits remote code execution on systems running a vulnerable version of Crowd or Crowd Data Center.

EVRS 92/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.954 99.87th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · listed over a year
--	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.954 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified
CISA required action: Apply updates per vendor instructions.
 Basis: CISA KEV required action

All versions of Crowd from version 2.1.0 before 3.0.5 (the fixed version for 3.0.x), from version 3.1.0 before 3.1.6 (the fixed version for 3.1.x), from version 3.2.0 before 3.2.8 (the fixed version for 3.2.x), from version 3.3.0 before 3.3.5 (the fixed version for 3.3.x), and from version 3.4.0 before 3.4.4 (the fixed version for 3.4.x) are affected by this vulnerability.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
crowd	≥ 2.1.0 < 3.0.5 ≥ 3.1.0 < 3.1.6 ≥ 3.2.0 < 3.2.8 ≥ 3.3.0 < 3.3.5 ≥ 3.4.0 < 3.4.4	3.0.5 · 3.1.6 · 3.2.8 · 3.3.5 · 3.4.4	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-8977-4jwc-24g8	Additional guidance	jira.atlassian.com/browse/CWD-5388
NVD	nvd.nist.gov/vuln/detail/CVE-2019-11580	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-3250	Current data	evulnable.com/vulnerability-management/cve/CVE-2019-11580

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.